ico.
Information Commissioner's Office

Risk Management Policy and Appetite Statement

1. Risk Management Executive Summary

1.1. This risk management policy and appetite statement forms part of the Information Commissioner's Office's (ICO's) internal control and corporate governance arrangements. This policy, and the adoption of the overall risk management framework, including allocating proportionate resources to risk management, is owned by the Chief Operating Officer. Risk Management must be embedded into the ICO's culture and all of its activities, as such, all staff have a role to play to ensure the ICO's risk management framework is effective. A summary of roles and responsibilities in relation to risk management is detailed in the ICO's Risk and Opportunity Management Procedure.

1.2. The purpose of this policy is to clearly outline the ICO's commitment to risk management, describe the goals and objectives of risk management, and provide a framework for continuing to embed risk management across the organisation, with defined roles and responsibilities and a structured process. It sets out the commitment from the Commissioner and ICO senior managers to managing risks effectively across the ICO, and the standard of risk management we deliver across the ICO. It sets the tone for the organisation and increases the likelihood that the management of risk will be given appropriate consideration by all.

1.3. As the ICO looks forwards, even in a short period of time there will be a host of factors which influence the nature of the ICO's regulation duties and the environment in which it operates. These factors challenge the ICO to continually review its systems and approaches, and to experiment with new ideas allowing mixed and flexible use of resources. The Commissioner and ICO senior managers and decision makers, will all face existing, new and evolving risks to achieving the ICO's objectives. This will be against a backdrop of a constantly evolving environment, with a need to continually adapt internal organisation to meet technological and social changes, new legal requirements and economic challenges.

1.4. Our three core values: ambitious, collaborative and service focused are central to risk management. They influence our risk culture, the way we plan, make decisions, how we behave towards one another and continually challenge ourselves to achieve our vision.

1.5. Effective risk management is not about avoiding all risk: with an effective risk management culture and strengthened understanding of risk management we may decide to take more risks in some areas of the organisation. This will always be on an informed basis, ensuring that the benefits of the risk-taking enable us to achieve our ambitions and help us to innovate as effectively and cost efficiently as possible, as we continue to achieve the goals of our Information Rights Strategic Plan (IRSP) and underpinning strategies and plans.

1.6. Through the implementation and embedding of an effective risk management framework, and the setting of an appropriate risk appetite, we will ensure that we are ideally placed to achieve our objectives as a regulator and to uphold information rights in the public interest.

2. Introduction

2.1. A risk is an expression of uncertainty to achieving objectives and can be a threat or an opportunity. A threat is a possible future event or action which will adversely affect the ICO's ability to achieve its goals, priorities and objectives and to successfully deliver approved strategies. An opportunity is an event or action that will enhance the ICO's ability to achieve its goals, priorities and objectives and deliver approved strategies. Risk is part of everything we do. Managing risk improves the way we deliver our services. It is acknowledged that some risks will always exist and will never be eliminated, but through risk identification we anticipate eventualities and it helps us to respond to changes in need and to prepare response plans where we can. This ensures that we can minimise the likelihood of a risk occurring as far as possible, or minimise the impact if it does happen.

2.2. The ICO will manage risk (both threats and opportunity), effectively and in a consistent manner in all aspects of its business including planning, delivering, operating and overseeing programmes and performance. All management levels will develop and encourage a culture of well-informed risk-based decision making. Managing risk will be at the core of the ICO's governance, enabling sound strategic and operational decision making and good business management. Risks are focused on how they effect our ability to deliver objectives. To enable this, we hold risk registers at various levels, such as: a corporate risk register for risks which effect our ability to achieve corporate objectives; Directorate risk registers for risks which effect our ability to achieve Directorate objectives; and project risk registers, for risks which effect our ability to achieve the objectives of the specific project.

2.3. There are 4 goals detailed below which outline the ICO's approach to risk management and internal control.

3. Goal#1: Risk Governance: Risk management will be embedded into the ethos, culture, policies and practices of the ICO so that risk management is an integral part of decision making, management and governance practices.

3.1. Considering and responding to existing and new threats, and the ability to recognise and seize new opportunities, is fundamental to achieving the ICO's desired goals and key strategic priorities. Underlying this is a commitment from the ICO to transparency and good governance. Decisions made by the ICO are evidence-based and subject to appropriate challenge. This requires high standards of corporate governance. Effective risk management is a key principle of corporate governance and a key contributor to a sound control environment.

3.2. Risk management plays a key role in helping us achieve our goals and priorities. It helps ensure decision-making is better informed, ensures public resources are used efficiently and helps us to avoid unwelcome surprises.

3.3. The following actions will help us to achieve Goal#1:-

Action: We will ensure the effectiveness of the ICO's risk management framework, so that the Commissioner, Management Board and ICO senior management are able to rely on adequate three lines of defence functions. This includes monitoring and assurance functions undertaken by the Audit and Risk Committee and the Risk and Governance Board.

Action: We will ensure that good risk management is an integral part of everyday governance business, including policy making, decision making, performance management, business planning and assurance activity.

Action: We will ensure that internal audit coverage is driven by a clear understanding of the risks, challenges and opportunities facing the ICO. Some of the risks will be unique to individual service areas within the ICO; others will be common to other regulators and organisations, giving opportunities for benchmarking.

4. Goal#2: Risk Culture: We will ensure we have an organisational culture which empowers staff to undertake well-managed risk-taking and are able to escalate risks and concerns.

4.1. A strong risk culture is one that expresses its values and defines expected behaviours. Staff understand how cultural attributes are measured and its values are aligned with reward processes.

4.2. The following actions will help us to achieve Goal#2:-

Action: ICO senior management will lead by example with a combination of positive attitudes, behaviours and activities to create an environment where consideration of risk is part of everything we do.

Action: ICO senior managers will lead by example by taking ownership and being accountable for Corporate and Directorate level risks, ensuring that effective and proportionate action is taken to mitigate those risks so that we can achieve our objectives

Action: We will encourage service excellence and innovation, taking considered risks; and, engender a continuous improvement mind-set towards the way we manage risk, and implement learning lessons, and in doing so, improve delivery of our regulatory services.

Action: We will promote open, honest and collaborative discussions about our risks and encourage a no-blame risk environment and culture.

Action: We will communicate clear messages, ensuring everyone understands the role they have to play in identifying and managing the risks and opportunities we face in the successful delivery of our strategic plans, projects, and day to day service delivery business objectives.

5. Goal#3: Risk Skills: We will ensure that staff have the skills and knowledge they need to fulfil their risk management responsibilities.

5.1. Educating staff is particularly important in risk management to have an effective risk framework in place. The greatest risks tend to be related to people and our people are also our greatest control mechanism. This includes understanding of the organisational risk appetite, as well as risk management practices.

5.2. The following actions will help us to achieve Goal#3:-

Action: We will equip ICO staff with the tools, skills and time they need to fulfil their risk management responsibilities. This will include the provision of training, guidance, templates, and by allowing time on meeting agendas for risk discussion.

Action: We will encourage and support staff in identifying and discussing risk in their everyday business; and to pro-actively deal with risks that come to their attention.

Action: We will provide opportunities for shared learning on risk management across the ICO and with other regulators, partners and stakeholders where appropriate.

6. Goal#4: Risk Management Approach: The ICO will successfully manage risks and opportunities at all levels – strategic, operational, programme, project and in collaboration activity, so that it increases the probability of achieving its goals and priorities.

6.1. Accountability for service delivery brings with it responsibility for identifying, assessing, owning, managing and communicating key risks to service delivery. This requires the collaborative effort of our management, all our staff and any key partners.

6.2. The following actions will help us to achieve Goal#4:-

Action: We will adopt a consistent application and embed an agreed business risk management approach throughout the ICO establishing a risk and opportunity management procedure which clearly defines the roles, responsibilities and reporting lines within the ICO for risk management.

Action: We will integrate the management of risk into all of our business processes, including (but not limited to) regulatory, finance, planning, performance management, key decision-making processes, project and programme management and major change initiatives.

Action: We will maintain a hierarchy of risk registers, that are regularly reviewed and monitored to ensure that key risks are visible, are owned at the right level of the organisation, and are actively addressed. We will ensure that risks are escalated or de-escalated appropriately between the risk registers, and will ensure that cross-cutting risks identified in multiple registers are appropriately managed.

Action: We will use national and best practice guidelines on risk management and engage in relevant risk management forums and benchmarking exercises to identify further opportunities for improvement in our approach to risk management.

7. Internal Control and Risk Management

7.1. The system of internal control incorporates risk management. This system encompasses a number of elements that together facilitate an effective and efficient operation, enabling the ICO to respond to a variety of operational risks.

7.2. These elements include:-

a. Policies and procedures: Attached to significant risks are a series of policies that underpin the internal control process. The policies are approved and implemented and communicated by senior management to staff. Written procedures support the policies where appropriate.

b. Planning and Performance Management: By integrating risk management with the ICO's strategic, regulatory and financial planning, budgeting and performance management processes and individual service and business delivery plans we are able to monitor risks to achieving the objectives, determine which risks have the most significant impact, recognise where risks are increasing or decreasing and prioritise resource accordingly.

c. Horizon Scanning: This approach to risk management informs the ICO's business processes, and includes regular risk horizon scanning through strategic planning, including the strategic threat assessment and work of the intelligence team; service and business planning and performance, policy making and review work undertaken by the Regulatory Futures Directorate, as a core part of their business area. Horizon scanning for risks is also undertaken through our programme and project work and through partnership working and collaboration with other regulators and public bodies. We also make good use of our networking arrangements and relationship with both our internal and external auditors to stay alert to new and emerging risks

d. Reporting and Annual Report: Comprehensive bi-monthly reporting is designed to monitor key risks and their controls. Decisions to rectify problems are made at regular meetings of the Executive Leadership Team. The Audit and Risk Committee's Annual Report includes a review of the effectiveness of the internal control system. The Risk and Governance Board reviews corporate risks at every meeting.

e. Strategic Threat Assessment (STA): The STA aims to support ICO decision-makers to prioritise and direct our resources, relationships and regulatory effort. The STA also aims to assist staff to identify and share actionable intelligence across the organisation and externally. It is linked to the Information Rights Strategic Plan (IRSP) and the Regulatory Action Policy (RAP) (incorporating our regulatory priorities).

f. Information Governance Group: The Information Governance Group (IGG) is responsible for the overview and scrutiny of information governance (IG) arrangements and for making recommendations to the Risk and Governance Board and the Senior Information Risk Owner (SIRO) on information governance decisions. The Group provides assurance that; an effective and efficient IG framework is in place, that the ICO is compliant with regulations; and that information governance risk is well managed across the organisation.

g. Business Continuity: The business continuity process is essentially risk management applied to the whole organisation and its ability to continue with its service provision in the event of a catastrophic event. The ICO has developed a complimentary Business Continuity Policy to Risk Management alongside its corporate Business Continuity Plan.

h. Anti-Fraud: The ICO has a fraud response plan, which directs staff towards ensuring a professional and ethical approach to combating fraud.

i. Whistleblowing: The ICO is committed to the highest possible standards of openness, probity and accountability. Employees, contractors, suppliers to or consultants with, the ICO are often the first to realise that something wrong may be happening within. "Speak up", the ICO's Whistleblowing Policy and Procedure is intended to help those who have concerns over any potential wrong-doing within the ICO.

j. Audit and Accreditation reports: The ICO makes reference to and acts upon the results of the work of the internal and external auditors and on information and recommendations received from other feedback mechanisms, including governments, professional bodies and accreditation bodies.

8. Information Commissioner's Office Risk Appetite Statement

8.1. This risk appetite statement sets out how the ICO balances threats and opportunities in pursuit of achieving its objectives. Understanding and setting a clear risk appetite level is essential to achieving an effective risk management framework. Establishing and articulating the risk appetite level helps to ensure that the ICO responds to risk consistently, in line with a shared vision for managing risk. Public sector organisations cannot be risk averse and be successful. There are risks facing the ICO such as legal compliance where its risk appetite may be very low. Conversely there are risks with choices about change and development, projects, research and delivery roles, where some risk taking is expected. The risk appetite sets out the level of residual risk which is tolerable: where the risk appetite is low, we will either choose options which have low inherent risk, or devote more resources into making sure that we have fully mitigated the inherent risks of the option we want to pursue; where the risk appetite is high, we are more likely to choose options with a high degree of inherent risk or devote less resources to mitigating the risks.

8.2. The risk appetite statement forms a key element of the ICO's assurance and governance framework and is set by the Commissioner and their Management Board. Breaches of risk appetite, or tensions arising from its implementation will be dealt with by the Executive Team or Risk and Governance Board as appropriate. These may reflect a need to review the risk appetite statement. In determining the statement it is recognised that risk appetite is subject to change and needs to flex in line with the organisation's strategic environment and business conditions; and as such the statement will be reviewed on a regular basis and at least annually.

8.3. The ICO distinguishes between those risks which are mostly operational in nature (and as such are within our control) and those external risk factors which are not directly within our control but which nevertheless must be identified and considered to address those risks we can influence or contingency plans we need to make. This will be discussed and escalated through internal line management chains.

9. Overarching Risk Appetite Statement

9.1 The organisation does not have a single risk appetite, but rather appetites across the range of its activities. The ICO recognises that in pursuit of its IRSP goals, strategic priorities and outcomes that it may choose to accept different degrees of risk in different areas. The ICO has established and articulated risk appetite for the differing areas of its business (see below). Where the ICO chooses to accept an increased level of risk it will do so, subject always to ensuring that the potential benefits and threats are fully understood before actions are authorised, that it has sufficient risk capacity, and that sensible and proportionate measures to mitigate risk are established.

10. Risk Appetite Definitions

10.1. The ICO's risk appetite definitions are as follows:-

Appetite	Rank	Description
Hungry	5/5	Eager to be innovative and choose activities that focus on maximising opportunities (additional benefits and goals) and offering potentially very high reward, even if these activities carry a very high residual risk.
Open	4/5	Undertakes activities by seeking to achieve a balance between a high likelihood of successful delivery and a high degree of reward and value for money; or activities themselves may potentially carry, or contribute to, a high degree of residual risk.
Cautious	3/5	Willing to accept/tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant reward and/or realise an opportunity; or Activities undertaken may carry a high degree of inherent risk that is deemed controllable to a large extent.
Minimalist	2/5	Predilection to undertake activities considered to be very safe in the achievement of key deliverables or initiatives; or activities will only be taken where they have a low degree of inherent risk. The associated potential for reward/pursuit of opportunity is not a key driver in selecting activities.
Averse	1/5	Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is paramount; or activities undertaken will only be those considered to carry virtually no inherent risk.

11. Business Area Risk Appetite Levels

11.1. The ICO's risk appetites across a range of activities are articulated as follows:-

a) Legal (legislation and regulatory advice): The public sector is undergoing reform, involving new legislation, new legal frameworks, the creation of new delivery models, and new entities for the ICO to engage with. We are regulated and we are also regulators. Where we are working with relatively untested legislation (or working towards changes to legislation) we are willing to adopt an **open** risk appetite to achieve our statutory objectives and to determine the extent of our powers and our jurisdiction.

b) Legal (compliance): We retain an **averse** risk appetite to behaving in an illegal, unrealistic or irrational way, or any other way, which would be likely to give rise to a successful judicial review.

c) Information Governance: We are heavily reliant upon information and data to be able to operate as an effective risk-based regulator. The accidental or deliberate wrongful disclosure of sensitive or official information has the potential to erode trust, damage our reputation and ultimately prevent us from being able to function. As such we have **minimal** appetite for such risks. The accidental or deliberate wrongful disclosure of sensitive or restricted information has the potential to erode trust, damage our reputation and ultimately prevent us from being able to function.

d) Anti-fraud and financial controls: We are **averse** to the risks of internal fraud and fraudulent behaviour and will maintain appropriately robust controls and sanctions to maximise prevention, detection and deterrence of this type of behaviour.

e) Security: Alongside other businesses we recognise that the ICO faces increasing physical and information security and cyber risks which may be internal or external to the organisation and may be malicious or unintentional. The ICO is risk **averse** to these risks which may potentially cause loss, harm or reputational damage related to the ICO's physical and technical infrastructure and assets, or the use of technology within the organisation. We place an emphasis on deploying our security controls effectively against a baseline risk appetite of averse.

f) Operational controls and compliance: In acknowledgement of the growth and operational maturity of our multiple regulatory services, we maintain a **cautious** risk appetite towards sustaining appropriate operational processes, systems and controls to support the provision of our public services.

g) Organisational controls and compliance: As a public sector organisation the ICO has a wide range of statutory obligations which it must show compliance. We maintain a **minimalist** risk appetite towards the processes, systems and controls to ensure that we fulfil these obligations.

h) Organisational change and development: We adopt a more **open** appetite for the development and enhancement of our systems and services, including new uses of technology.

i) Reputational: We rely on our reputation to influence and secure the engagement of those we regulate and other stakeholders. The support of these parties is essential to achieving our goals and so we hold a strong commitment to being seen as a proportionate and respected regulator and retain an overall **cautious** risk appetite with regard to our reputation. However, we are prepared to take a stance which may be opposed by some of our audience where we believe it is necessary for the achievement of one or all of our statutory objectives.

j) Staff recruitment: We are committed to attracting the highest calibre of candidates to the ICO to maximise the personal and collective contributions of staff towards the achievement of our strategic vision and goals. We take a **hungry** approach, actively seeking new and innovative ways to maximise our recruitment reach so that our candidate pool is as diverse and capable as it is possible to be.

k) Staff retention, development and progression: We are committed to providing a working environment in which all ICO employees are able to progress, develop and thrive, working positively and constructively to maximise their potential and career development. We will take an **open** approach, seeking to tailor our approaches to the needs of individual staff or particular professions or departments.

l) Staff performance: We are committed to providing a working environment in which all ICO employees are able to maximise their personal and collective contributions towards the achievement of our strategic vision and goals. When we identify poor performance we will take a **cautious** approach, seeking to provide the opportunity and support to enable performance to improve. However, when we identify good performance we will take a more **open** approach, ensuring our reward and recognition mechanisms amplify ICO employee productivity to retain high calibre employees.

m) Staff misconduct: We are **averse** to risks of misconduct from staff, and will tackle these. We aim to act clearly and effectively to maintain the high standards of professional conduct and behaviour we expect of our workforce.

n) Regulatory guidance and strategy: We have a **hungry** appetite when taking proportionate risks or committing to take maximum advantage of opportunities which help us to achieve our strategic regulatory goals.

o) Regulatory evaluation (risks to the public): We have a **cautious** risk appetite in evaluating decisions to commence and dedicate resource to regulatory investigations and interventions to address risks to the public, based on the principles set out in the Regulatory Action Policy and the extent to which it furthers our strategic objectives.

p) Regulatory evaluation (supporting innovation): We have an **open** risk appetite in evaluating decisions to commence and dedicate resource to regulatory investigations and interventions regarding products which support safe innovation.

q) Regulatory prioritisation: We have an **open** appetite towards risks in prioritising work based on particular public benefits, or likelihood of positive impact, rather than focusing on order in which they were reported to the ICO.

r) Regulatory investigation: We will conduct our regulatory investigations, audits, engagement and research to address risks to the public in line with clear internal policies and procedures and our prioritisation framework wherever appropriate and have an **open** risk appetite in this area to maximise the impact that we can have.

s) Regulatory enforcement: We will assess the likely impact of each decision on taking potential regulatory action is based on the evidentiary findings of investigations and will take a **cautious** approach to risk in this area.

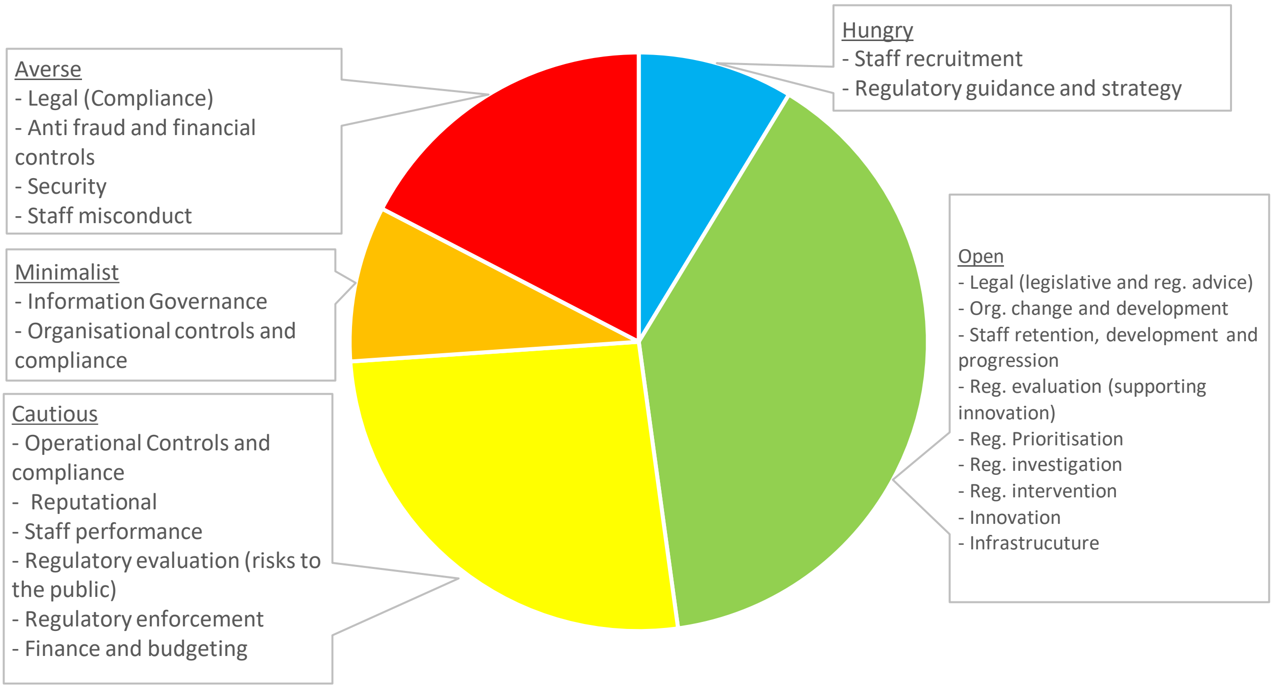
t) Regulatory intervention: We will use our formal powers to better understand and evaluate risk to consumers or the economy and will take an **open** approach to risk in this area.

u) Innovation: We have an **open** appetite for taking well managed risks where innovation and change create opportunities for discernible benefits and clear improvements in our ability to achieve our strategic vision and goals.

v) Finance and budgeting: as a responsible public sector organisation we need careful financial planning to ensure that we do not risk significant over-spend or under-spend. Therefore, we have a **cautious** risk appetite in this area.

w) IT, accommodation, staffing resources and other infrastructure: as we are a publicly funded organisation, we need to ensure that we maximise our impact and value for money. Therefore we have an **open** risk appetite towards our development in these areas.

12. Risk Appetite Heat Map



13. Risk Capacity

13.1. The ICO's risk capacity is determined through understanding its risk environment in the following areas:-

- Reputation – can the ICO withstand pressures as they arise as a result of the activity
- Financial – is there sufficient financial contingency for the activity

- Political – what political tolerance is there for any adverse risk events materialising both internally and externally
- Regulatory – what pressures does the activity place on the ICO's regulatory position
- Infrastructure –is there sufficient infrastructure to manage risk
- People – are there sufficient trained and skilled individuals
- Knowledge - is sufficient knowledge available to the ICO

14. Risk Tolerance and Thresholds

14.1. As described above, the risk appetite is the broad description of the amount of risk the ICO is willing to accept or retain in order to achieve its objectives. It is a statement or series of statements that describe the organisation's attitude towards risk taking.

14.2. The risk tolerance uses the risk appetite to inform:-

- expectations for mitigating, accepting and pursuing specific types of risk
- boundaries and thresholds of acceptable risk taking
- actions to be taken or consequence for acting beyond approved tolerances such as escalation procedures

14.3. A tolerance level is set for each risk to identify the level at which the risk can be accepted, rather than needing further mitigation to reduce the risk. This will be aligned to the risk appetite: risks in areas with a more averse risk appetite will have a lower tolerance score than risks in areas with a more hungry risk appetite. The tolerance level should be set as part of the creation and initial scoring of the risk, and should be reviewed as part of the regular review of each risk.

14.4. Tolerance levels will be established for organisational activities at different levels across the ICO as appropriate in line with the risk appetite. Mitigating actions to bring the risk in line with the tolerance score should be funded from Directorate budgets, in line with agreed budgeting procedures.

15. Document History

Version	Date	Approved by	Ref
3.0	08/01/2020	Deputy Chief Executive Officer	EmailMinute
3.1	13/01/2020	Executive Leadership Team	Minute
3.1	20/01/2020	Audit Committee	Minute
3.1	24/01/2020	Management Board (subject to amendments)	Minute
3.2	11/02/2020	Management Board (amendments agreed on 24/1/20)	Minute
4.0	08/12/2020	Risk and Governance Board	Minutes
4.1	10/1/22	Audit and Risk Committee	Minutes
4.2	21/3/22	Management Board (amended risk appetite agreed on 21/3/22	Minutes